

08/868337

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS & REGISTRATION

PCT/FI 99 / 0 10 36

11 JAN 2000

Helsinki 15.12.1999

6/L

REC'D 26 JAN 2000

WIPO

PCT

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT



Hakija
Applicant

Sonera Oy
Helsinki

Patenttihakemus nro
Patent application no

982728

Tekemispäivä
Filing date

16.12.1998

Kansainvälinen luokka
International class

G07F

Keksinnön nimitys
Title of invention

"Menetelmä ja järjestelmä digitaalisen allekirjoituksen toteuttamiseksi"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Pirjo Kaila
Tutkimussihteeri

PRIORITY DOCUMENT

Best Available Copy

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5204
Telefax: + 358 9 6939 5204

1
2**MENETELMÄ JA JÄRJESTELMÄ DIGITAALISEN ALLEKIRJOITUKSEN
TOTEUTTAMISEKSI**

Esillä oleva keksintö liittyy tietoliikenne-
järjestelmiin ja digitaalisen tiedon allekirjoitus- ja
5 salaustekniikkaan. Erityisesti keksintö liittyy uuden-
tyyppiseen ja kehittyneeseen menetelmään ja järjestel-
mään, jonka avulla lomake tai muu allekirjoitettava
sähköisessä muodossa oleva tieto voidaan allekirjoit-
taa ja varmistua allekirjoituksen ja allekirjoittajan
10 oikeellisuudesta.

TEKNIIKAN TASO

Entuudestaan on tunnettua käyttää digitaalis-
ta matkaviestintä, kuten GSM-järjestelmän (Global Sys-
tem for Mobile Communications, GSM) matkaviestintä,
15 kaupallisiin transaktioihin, kuten laskun tai maksun
maksamiseen sähköisesti. Patenttijulkaisusta US
5,221,838 tunnetaan laite, jota voidaan käyttää maksa-
miseen. Julkaisussa on kuvattu sähköinen maksujärjes-
20 telmä, jossa maksupäätteenä käytetään langattomaan
ja/tai langalliseen tiedonsiirtoon kykenevää päätelai-
tetta. Julkaisun mukaiseen päätelaitteeseen kuuluu
kortinlukija, näppäimistö, ja viivakoodin lukija tie-
tojen syöttämiseksi ja näyttö maksuinformaation esit-
25 tämiseksi.

Patenttijulkaisusta WO 94/11849 tunnetaan me-
netelmä tietoliikennepalveluiden käyttämiseksi ja mak-
suliikenteen suorittamiseksi matkapuhelinjärjestelmäl-
lä. Julkaisussa kuvataan järjestelmä, johon kuuluu
30 päätelaite, joka on yhteydessä televerkon kautta pal-
veluntarjoajan keskustietokoneeseen, joka sisältää
palveluntarjoajan maksujärjestelmän. Matkapuhelinver-
kon päätelaitteeseen eli matkaviestimeen voidaan lisä-
tää tilaajan tunnistusyksikkö, joka käsittää tilaaja-
35 tiedot tilaajan tunnistamiseksi ja teleliikenteen sa-
laamiseksi. Tiedot voidaan lukea päätelaitteeseen käy-

tettäväksi matkaviestimissä. Esimerkkinä julkaisussa mainitaan GSM-järjestelmä, jossa käytetään SIM-korttia (Subscriber Identity Module, SIM) tilaajan tunnistusyksikkönä.

- 5 Julkaisun WO 94/11849 mukaisessa järjestelmässä matkaviestin on yhteydessä matkapuhelinverkon tukiasemaan. Julkaisun mukaan yhteys muodostetaan edelleen maksujärjestelmään ja maksettava määrä samaten kuin tilaajan tunnistamiseen tarvittava data välitetään maksujärjestelmään. Julkaisussa kuvatussa pankkipalvelussa asiakas asettaa pankin palvelukortin, joka sisältää SIM-yksikön, GSM-verkon päätelaitteeseen. Puhelinperustaisessa pankkipalvelussa päätelaite voi olla standardin mukainen GSM-matkaviestin. Julkaisussa 15 kuvatulla menetelmällä voidaan käyttää langatonta tietoliikenneyhteyttä maksujen ja/tai laskujen tai muiden vastaavien pankkipalvelujen tai kassapalvelujen toteuttamiseen.

- Ongelmana yllä mainituissa ratkaisuihin on, 20 että niissä ei oteta kantaa maksun luotettavuuteen maksajan ja maksun saajan kannalta. Käytettäessä matkaviestintä maksamiseen on tärkeää, että sekä maksaja että maksun saaja voivat luottaa järjestelmään. Maksajan on tarkkaan tiedettävä, mistä maksaa, minkä verran maksaa, kenelle maksaa, miten maksaa jne. Maksun saajan on myös tarkkaan tiedettävä, kuka maksaa, mistä maksaa, minkä verran maksaa jne. 25

- Kuten tiedetään, tiedon siirtäminen paikasta toiseen sähköisessä muodossa on helppoa. Sen sijaan 30 vaikeampaa on varmistua siitä, että siirretty tieto säilyy siirron aikana muuttumattomana ja siitä, että esimerkiksi matkapuhelimen näytöllä esitetty tieto lähetetään juuri sellaisenaan ja muuttumattomana vastaanottajalle.

- 35 Entuudestaan on tunnettua käyttää tiivistettyä, joka on lähetettävästä tiedosta muodostettu ja laskettu tietokenttä. Tiivisteen laskemiseen käytetään

yleensä algoritmia, joka on yksisuuntainen funktio eli tiivistämisestä ei ole mahdollista selvittää sen muodostamiseen käytettyjä tietoja. Eräs käytettävä algoritmi voi olla SHA-1 (Secure Has Algorithm).

- 5 Digitaalisella allekirjoituksella, jota pidetään yleisenä vaatimustasona sähköisessä maksamisessa, varmistetaan välitettävän aineiston eheys ja lähettäjän alkuperä. Digitaalinen allekirjoitus muodostetaan salaamalla välitettävästä aineistosta laskettu tiiviste 10 lähettäjän salaisella avaimella. Koska kukaan muu ei tunne lähettäjän salaista avainta, voi vastaanottaja purkaessaan salauksen lähettäjän julkista avainta käyttäen varmistua siitä, että aineisto on muuttumaton ja lähettäjän muodostama. Eräs esimerkki digitaalisessa 15 allekirjoituksessa käytettävästä algoritmista on RSA-salausalgoritmi, joka on julkisen ja salaisen avaimen salausjärjestelmä ja jota käytetään myös viestien salaamiseen.

20 KEKSINNÖN TARKOITUS

- Esillä olevan keksinnön tarkoituksena on poistaa edellä esitetyt ongelmat. Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin uuden tyyppinen menetelmä ja järjestelmä lomakkeen tai muun 25 vastaavan tiedon allekirjoittamiseksi matkaviestimellä. Tässä yhteydessä lomakkeella voidaan tarkoittaa monen tyyppistä ja -sisältöistä sähköisesti tulkittavissa olevaan viestiä, sanomaa tai tietorakennetta. Lomake voi olla olio- tai ohjelmisto-objekti - 30 tyyppinen informaatio, jota voidaan käsitellä sähköisessä muodossa.

- Edelleen keksinnön tarkoituksena on tuoda esiin yksinkertainen ja helposti nykYTEKNIikkaan implementoitavissa oleva menetelmä kaupallisten transaktioiden, kuten laskun maksamisen ja pankkiasioinnin, 35 toteuttamiseksi matkaviestimellä.

KEKSINNÖN KOHDE

Keksinnön kohteena on menetelmä sähköisessä muodossa olevan lomakkeen, joka määriteltiin yllä, digitaaliseksi allekirjoittamiseksi turvallisesti käyttäen matkaviestintä tai muuta vastaavaa ja siihen verrattavissa olevaa laitetta. Menetelmässä siirretään allekirjoitettava aineisto, joka voi käsittää ainakin lomakkeen, sen tunnisteiden, jaetun datan, ja/tai lomakkeeseen lisätyt olennaiset tiedot, matkaviestimeen. Allekirjoitettava aineisto voidaan muodostaa myös lomakkeen tunnisteesta ja lomakkeeseen liittyvistä olennaisista tiedoista, esimerkiksi lomakkeen ollessa pankkisiirtolomake, voidaan aineisto muodostaa pankkisiirtolomakkeen tunnisteesta ja lomakkeen olennaisten kenttien tiedoista, kuten maksajasta, saajasta ja summasta.

Keksinnön mukaisesti lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste edullisesti ennen aineiston siirtämistä matkaviestimeen. Tiiviste lisätään aineistoon siirrettäväksi, jolloin sitä voidaan käyttää apuna tarkistuksen suorittamisessa. Kun aineisto on siirretty matkaviestimeen, se allekirjoitetaan matkaviestimessä ja edelleen keksinnön mukaisesti allekirjoitetun ja siirretyn aineiston oikeellisuus ja vastaavuus varmistetaan vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään. Allekirjoittaminen voidaan tehdä myös siten, että allekirjoitetaan sekä olennaiset tiedot ja tiiviste, jolloin varmistetaan vielä siitäkkin, että matkaviestimellä allekirjoitettu aineisto vastaa allekirjoitettavaksi siirrettyä aineistoa.

Kun kysymyksessä on tietyn tyyppiset sovellukset, kuten maksusovellukset, voidaan matkaviestimeen siirretty aineisto siirtää myös toiselle osapuolelle, esimerkiksi pankille, joka voi laskea saamas-

taan aineistosta tiivisteen. Matkaviestimestä allekirjoitettu aineisto voidaan edelleen salata ja siirtää salattu ja allekirjoitettu aineisto matkaviestimestä myös toiselle osapuolelle. Toinen osapuoli purkaa sa-

5 lauksen, tarkistaa allekirjoituksen, laskee matkaviestimestä saamastaan aineistosta toisen tiivisteen ja vertaa tätä ensimmäiseen alkuperäisestä aineistosta laskemaansa tiivisteseen. Jos toinen osapuoli hyväksyy digitaalisen allekirjoituksen ja jos ensimmäinen

10 ja toinen tiiviste vastaavat toisiaan, pankki hyväksyy matkaviestimellä tehdyn allekirjoituksen. Kun pankki on hyväksynyt allekirjoituksen, se voi merkitä allekirjoitettuun ja purettuun aineistoon aikaleiman ja arkistoida aineiston allekirjoitustapahtuman.

15 Edellä on kuvattu menettely, jossa asiakas allekirjoittaa pankille pankilta saamansa lomakkeen. Asiakas tai matkaviestimen käyttäjä voi olla yhteydessä paikallisesti maksuautomaattiin tai vastaavaan, jolloin maksuautomaatti välittää asiakkaalle maksettavaksi ja hyväksyttäväksi tarkoitetun lomakkeen. Tällöin asiakas käy sanomavaihtoa maksuautomaatin kanssa paikallisesti ja maksuautomaatti välittää digitaaliset allekirjoitustiedot edelleen. Kuitenkin maksuautomaatti voi välittämästään liikenteestä päätellä asiakkaan

25 hyväksyneen sille tarjotun palvelun ja maksulomakkeen. Tällöin automaatti voi palvella asiakasta tämän haluamalla ja maksamalla tavalla paikallisesti odottamatta välttämättä pankilta hyväksyntää siitä. Tilanne vastaa käytännössä normaalia käytäntöä, jossa esimerkiksi

30 kaupan kassalla asiakas pankkikortillaan maksaa tuotteet tai palvelut, ja kauppa tarjoaa ne asiakkaalle varmistamatta maksun oikeellisuutta pankista.

Aineisto voidaan myös salata ennen sen siirtämistä matkaviestimeen, jolloin matkaviestimestä on

35 purettava salaus ennen aineiston allekirjoittamista. Tällä voidaan varmistaa se, että vain haluttu matka-

viestin vastaanottaa siirrettävän aineiston ja taata tietojen turvallisuus.

Lomakkeen muodostamiseen voidaan käyttää ennalta sovittua tunnisteellista lomakepohjaa, viestirakennetta tai mitä tahansa muuta sanomarakennetta, johon täydennetään ennalta sovitut oleelliset tiedot ennen lomakkeen siirtämistä matkaviestimeen. Tiiviste voidaan laskea esimerkiksi hash-funktiolla. Viestin ja/tai lomakkeen allekirjoitukseen ja/tai salaukseen voidaan käyttää julkisen ja salaisen avaimen menetelmää.

Keksinnön eräässä edullisessa sovelluksessa esitetään aineisto ja/tai osa siitä matkaviestimessä ennen aineiston allekirjoittamista. Esimerkiksi voidaan esittää lomakkeessa olevat saaja-, maksaja- ja viitetiedot sekä maksettava summa. Myös on mahdollista vaatia matkaviestimen käynnistämistä allekirjoitusmoodissa ennen aineiston siirtämistä siihen. Tämä voi käytännössä tarkoittaa sitä, että matkaviestimeen on syötettävä toinen ennalta määrätty PIN-koodi, jolla matkaviestin on konfiguroitu käynnistymään ennalta määrättyssä allekirjoitusmoodissa. Voidaan käyttää siis eräänlaista paikallista autentikointia.

Keksinnön kohteena on myös järjestelmä sähköisessä muodossa olevan lomakkeen digitaalisesti allekirjoittamiseksi turvallisesti matkaviestimellä. Järjestelmään kuuluu edullisesti maksuautomaatti ja siihen yhdistetyt välineet allekirjoitettavan aineiston, joka määriteltiin yllä, muodostamiseksi ja siirtämiseksi matkaviestimeen. Maksuautomaatilla voidaan tässä tarkoittaa mitä tahansa paikallista ja paikallisesti käytettävää automaattia, joka voi olla tietoliikenneverkon välityksellä yhdistetty palvelutarjoajaan, kuten pankkiin, kauppaan tai vastaavaan.

Maksuautomaatti voi olla toteutettu myös paikallisesti tietokoneeseen, joka on yhteydessä esimerkiksi Internet-verkon välityksellä palveluntarjoajaan,

jolloin palveluntarjoaja tarjoaa tuotteitaan ja palveluitaan Internet-verkon välityksellä. Tässä tapauksessa allekirjoitettava aineisto siirretään tietokoneelta allekirjoitettavaksi matkaviestimeen paikallista yhteyttä käyttäen tai suoraan palveluntarjoajan omalta palvelimelta käyttämättä paikallista tietokonetta ja yhteyttä.

Keksinnön mukaisesti maksuautomaattiin kuuluu välineet ensimmäisen tiivisteen laskemiseksi allekirjoitettavasta aineistosta. Samaten matkaviestimeen kuuluu allekirjoitusvälineet siihen siirretyn aineiston allekirjoittamiseksi. Allekirjoitusvälineisiin voi kuulua muisti, johon on tallennettu allekirjoituksen ja salauksen vaatimat algoritmit ja avaimet, ja prosessori, joka on yhdistetty muistiin ja joka käsittelee aineistoa toteuttaen digitaalisen allekirjoituksen ja mahdollisesti salauksen. Lisäksi maksuautomaattiin kuuluu välineet allekirjoitetun ja siirretyn aineiston oikeellisuuden varmistamiseksi vertaamalla matkaviestimessä allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään.

Järjestelmään voi myös kuulua palvelin, joka on yhdistetty maksuautomaattiin ja/tai matkaviestimeen ja joka on toisen osapuolen, kuten pankin tai luottokorttiyhtiön, valvonnassa. Tällainen palvelin voi siis olla esimerkiksi pankin ylläpitämä ja sitä voidaan käyttää pankkitapahtumien toteuttamisessa. Palvelimeen voi myös kuulua välineet matkaviestimen tekemän digitaalisen allekirjoituksen oikeellisuuden todentamiseksi ja salaus- ja purkuvälineet palvelimen ja maksuautomaatin ja/tai matkaviestimen välillä siirrettävän aineiston salaamiseksi ja purkamiseksi.

Palvelimeen voi kuulua myös välineet aikaleiman merkitsemiseksi aineistoon ja välineet aineiston allekirjoitustapahtuman arkistoinniseksi sen jälkeen, kun allekirjoitus on todettu oikeaksi. Nämä voi-

daan toteuttaa ammattimiehen sinänsä tuntemalla tavalla, eikä niitä sen vuoksi kuvata tässä tarkemmin.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksinnön ansiosta maksu-
5 sovellusten, varmistustapahtumien ja muiden toteuttaminen matkaviestimellä tulee entistä helpommaksi. Keksinnön ansiosta matkaviestintä voidaan luotettavasti käyttää digitaalisessa allekirjoituksessa ja tällöin digitaalinen allekirjoitus voidaan yhdistää monen eri
10 sovelluksen yhteyteen.

KUVALUETTELO

Seuraavassa keksintöä selostetaan edullisten sovellusesimerkkien avulla viittaamalla oheiseen piirustukseen, jossa:

kuvio 1 esittää erästä esillä olevan keksinnön mukaista edullista järjestelmää;

kuvio 2 esittää erästä toista esillä olevan keksinnön mukaista edullista järjestelmää;

20 kuvio 3 esittää vuokaaviomuodossa esillä olevan keksinnön erään edullisen sovelluksen; ja

kuvio 4 esittää kaaviomaisesti erään edullisen esimerkin allekirjoitettavan aineiston muodostamisesta esillä olevan keksinnön yhteydessä.

25 Kuviossa 1 esitettyyn järjestelmään kuuluu paikallinen maksuautomaatti (Local Payment Machine, LPM) 2 ja siihen yhdistetyt välineet allekirjoitettavan aineiston, käsittäen lomakkeen, sen tunnisteen, jaetun datan ja/tai siihen liitetyt olennaiset tiedot,
30 muodostamiseksi. Lisäksi maksuautomaattiin kuuluu siihen yhdistetyt välineet 4 aineiston siirtämiseksi matkaviestimeen. Vastaavasti matkaviestimeen kuuluu välineet 1, joilla matkaviestin (MS) kommunikoi maksuautomaatin kanssa. Eräessä edullisessa sovelluksessa välineet 1 ja 4 on toteutettu Bluetooth-teknologiaa käyttäen. Tarkempaa kuvausta Bluetooth-tekniikasta esitetään esimerkiksi WWW-sivulla www.bluetooth.com. Myös

muita tunnettuja siirtoyhteyskäytäntöjä, kuten infra-
 punaliitintää voidaan käyttää

Edelleen kuviossa 1 esitettyyn järjestelmään
 kuuluu palvelin 8, joka on yhdistetty TCP/IP-
 5 yhteydellä maksuautomaattiin 2 ja joka tässä esimer-
 kissä on pankin hallinnoima. Palvelimeen kuuluu edel-
 leen välineet 9 digitaalisen allekirjoituksen oikeel-
 lisuuden todentamiseksi - käytännössä niillä puretaan
 vastaanotetut salaviestit ja verrataan niissä olevia
 10 digitaalisia allekirjoituksia saatuihin käyttäjätie-
 toihin. Lisäksi palvelimeen kuuluu välineet 11 ja 12,
 joilla merkitään aikaleima allekirjoitettuun aineis-
 toon ja arkistoidaan allekirjoitustapahtuma sen jäl-
 keen, kun allekirjoitus on todettu oikeaksi. Vastaavat
 15 todentamisvälineet voivat kuulua myös maksuautomaat-
 tiin ja tässä ne on merkitty numerolla 7. Välineillä
 7, 11 ja 12 voi olla myös ominaisuus, jolla tarvitta-
 vat julkiset avaimet noudetaan esimerkiksi TCP/IP-
 verkon välityksellä yleisiltä avainhallintapalvelimil-
 20 ta.

Kuvion 1 esimerkissä siirretään salattu ai-
 neisto, johon kuuluu laskulomake ja laskulomakkeesta
 laskettu tiiviste H1 maksuautomaatilta 2 matkaviest-
 meen MS, vaihe 1. Matkaviestimessä aineisto eli lasku-
 25 lomake ja siihen tallennetut tiedot maksun saajasta,
 maksajasta, summasta ja maksun viitteestä esitetään
 matkapuhelimen näytöllä (10), josta matkaviestimen
 käyttäjä voi tarkistaa, mitä on allekirjoittamassa.
 Sen jälkeen käyttäjä allekirjoittaa matkaviestimellä
 30 MS aineiston ja siitä lasketun tiiviste H1. Aineis-
 to, johon on lisätty tiiviste H1, allekirjoitettuna
 digitaalisesti siirretään maksuautomaattiin 2, vaihe
 2. Maksuautomaatin 2 ja matkaviestimen MS välinen sa-
 nomaliikenne voidaan salata käyttäen matkaviestimen
 35 käyttäjän ja maksuautomaatin julkisia ja salaisia
 avaimia. Kun maksuautomaatissa 2 on tarkistettu alle-
 kirjoituksen oikeellisuus, lähetetään clearing-sanoma,

vaihe 3 maksuautomaatista edelleen pankkiin. Clearing on tunnettua ja yleisesti pankkimaaailmassa käytettyä tekniikkaa eikä sitä kuvata tässä tarkemmin.

Seuraavaksi viitataan kuvioon 2, jossa on
5 esitetty vastaavanlainen järjestelmä kuin kuviossa 1, mutta tässä järjestelmää käytetään hieman eri tavalla. Ensin maksuautomaatissa muodostettu aineisto, esimerkiksi lomake, siirretään pankkiin, vaihe 1. Sen jälkeen aineistosta lasketaan maksuautomaatissa tiiviste
10 H1, joka siirretään matkaviestimeen allekirjoitettavaksi, vaihe 2. Siirto voidaan tehdä käyttäen paikallista esimerkiksi Bluetooth-yhteyttä. Matkaviestimessä saatu sanoma allekirjoitetaan digitaalisesti ja sen jälkeen allekirjoitettu ja mahdollisesti salattu aineisto lähetetään pankkiin, vaihe 3. Pankissa verrataan maksuautomaatilta saadusta aineistosta laskettua tiivistettä H1 matkaviestimeltä saatuun tiivisteeseen H1_{an}, joka on digitaalisesti allekirjoitettu ja jos ne täsmäävät, hyväksytään allekirjoitustapahtuma. Tämän
20 jälkeen palvelimella tehdään aikaleimaus ja arkistoidaan saatu allekirjoitustapahtuma. Pankki voi olla myös muu vastaava palveluntarjoaja, kuten luottokorttiyhtiö, jolloin edellä kuvatun lisäksi allekirjoituksen oikeellisuus vahvistetaan pankille, maksuautomaatille tai muulle palveluntarjoajalle. Tällöin luottokorttiyhtiö vahvistettuaan allekirjoituksen ottaa vastuun tapahtumasta.

Viitaten vielä kuvioon 3 esitetään eräs keksinnön edullinen sovellus. Aluksi muodostetaan aineisto, joka on tarkoitettu allekirjoitettavaksi matkaviestimellä, lohko 31. Aineistosta lasketaan ensimmäinen tiiviste, H1, lohko 32. Sen jälkeen tarkistetaan, lohko 45, onko aineisto salattava ennen lähetystä matkaviestimeen. Jos aineisto on salattava, siirrytään
35 lohkoon 46 ja salataan se käyttäen matkaviestimen käyttäjän julkista avainta. Salauksen jälkeen siirrytään lohkoon 33. Jos aineistoa ei tarvitse salata,

siirrytään suoraan lohkoon 33, jossa aineisto siirretään matkaviestimelle. Seuraavaksi siirrytään lohkoon 34 ja tarkistetaan matkaviestimen näytöllä esitettävä aineisto tai sen olennaiset tiedot eli esimerkiksi laskun saajan ja maksun oikeellisuus. Jos maksaja hyväksyy, lohkossa 35, siirrytään lohkoon 37 ja allekirjoitetaan aineisto. Jos maksaja ei hyväksy lohkossa 35, siirrytään lohkoon 36, jossa lähetetään hylkäyssanoma aineiston lähettäjälle, esimerkiksi maksuautomaatille ja lopetetaan prosessi. Lohkosta 37 siirrytään lohkoon 38, jossa muodostetaan aineisto digitaalisesta allekirjoituksesta ja tiivistestä ja mahdollisesti saadusta aineistosta, johon kuuluu esimerkiksi lomakkeen olennaiset tiedot, lohko 38. Sen jälkeen aineisto siirretään maksuautomaattiin, lohko 39, josta edelleen siirrytään lohkoon 40 ja verrataan siirretystä aineistosta laskettua tiivistettä allekirjoitettuun tiivisteseen. Jos tiivistet vastavat toisiaan, lohko 41, hyväksytään allekirjoitus ja tehdään seuraavaksi määritellyt toimenpiteet.

Jos lohkossa 40 tiivistet eivät täsmänneet, voidaan proseduuri toistaa. Tässä vaiheessa on mahdollista käyttää laskuria, jolla tarkkaillaan sitä, ettei aineistoa lähetetä useammin kuin ennalta on sovittu. Lohkosta 40 siirrytään lohkoon 43, jossa kasvatetaan laskurin $k = k+1$ arvoa yhdellä ja siitä edelleen siirrytään lohkoon 44, jossa tarkistetaan laskurin arvo eli se, montako kertaa aineisto on siirretty matkaviestimeen. Jos arvo ylittää ennalta sovitun, siirrytään lohkoon 42 ja lähetetään hylkäyssanoma matkaviestimeen. Jos laskurin arvo on pienempi kuin ennalta sovittu, siirrytään uudelleen lohkoon 31 ja toistetaan prosessi.

Kuviossa 4 on esitetty eräs edullinen tapa muodostaa ja allekirjoittaa lomake tai aineisto digitaalisesti. Matkaviestimeen siirrettävään aineistoon kuuluu lomaketunniste, joka on yksilöllinen kaikille

käytettäville lomakkeille, lohko 51. Lomaketunnisteseen liittyy lomakekaavain, lohko 52, joiden perusteella sovellukset, asiakas ja sovelluksen tarjoaja tietävät tarkalleen, millaisesta lomakkeesta on kysymys. Aineistoa muodostettaessa lomaketunniste ja lomakekaavain ketjutetaan peräkkäin, kuten kuviossa 4 on esitetty ja sen jälkeen niistä lasketaan ensimmäinen tiiviste, lohko 54.

Lomakkeeseen liitetään usein lomakedataa, lohko 53, jo ennen sen siirtämiseksi matkaviestimeen allekirjoitettavaksi. Tällöin lomaketunniste ja lomakedata ketjutetaan peräkkäin kuvion 4 osoittamassa järjestyksessä ja niistä saatu bittijono edelleen ketjutetaan satunnaisten 16 tavun, lohko 55 kanssa. Niihin yhdistetään ensimmäinen tiiviste lohkosta 54.

Tässä vaiheessa aineisto on valmis siirrettäväksi matkaviestimeen, minkä jälkeen siitä lasketaan toinen tiiviste, lohko 56. Käytännössä toinen tiiviste lasketaan matkaviestimessä ja lisätään allekirjoitettavaan sanomaan, lohko 57. Samaten allekirjoitettavaan sanomaan on lisätty käyttäjädata, jota matkaviestimen käyttäjä on voinut täydentää omilla tiedoillaan tarpeen mukaan. Edullisesti myös tähän allekirjoitettavaan viestiin lisätään lohkosta 55 16 satunnaistavua, jolloin aineiston siirtäjän ja matkaviestimen käyttäjän muodostaman allekirjoitetun sanoman oikeellisuutta voidaan tarkistaa. Kun satunnaistavut käyttäjädata ja toinen tiiviste on asetettu peräkkäin, käyttäjän matkaviestimessä allekirjoitetaan sanoma digitaalisesti. Tämän jälkeen sanoma voidaan välittää eteenpäin toiselle osapuolelle, maksuautomaattiin tai muulle aineiston alkuperälähteelle.

Yhteenvetona todetaan vielä, että keksintönä on toteuttaa menetelmä ja järjestelmä, jossa käyttäjä, palvelun tarjoaja ja pankki, jotka mainitaan esimerkkinä, voivat varmistua digitaalisen allekirjoituksen oikeellisuudesta. Tarkoituksena on, että allekirjoit-

- tettava aineisto voidaan sitoa johonkin käyttäjän dataan, formaattiin ja käyttäjän tekemään digitaaliseen allekirjoitukseen. Allekirjoitus on siis pystyttävä sitomaan tietynlaiseen ketjuun, joka käytännössä vastaa nykyisin käytössä olevaa ketjua, jossa käyttäjä omalla manuaalisella allekirjoituksellaan hyväksyy ostoksiaan. Samaten menetelmän tarkoituksena on identifioida allekirjoittaja luotettavasti ja lainsäätäjän vaatimalla ja tarkoittamalla tavalla.
- 5
- 10 Esillä olevaa keksintöä ei rajata tässä esitettyihin esimerkkeihin, vaan monet muunnokset ovat mahdollisia pysyttäessä oheisten patenttivaatimusten määrittelemän suojapiirin rajoissa.

14

13

PATENTTIVAATIMUKSET

1. Menetelmä sähköisessä muodossa olevan lomakkeen digitaalisesti allekirjoittamiseksi turvallisesti matkaviestimellä, johon menetelmään kuuluu vaiheet

siirretään allekirjoitettava aineisto, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, matkaviestimeen, tunnettu siitä, että

lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste (H1);

lisätään tiiviste aineistoon siirrettäväksi matkaviestimeen;

allekirjoitetaan digitaalisesti matkaviestimellä siihen siirretty aineisto; ja

varmistetaan allekirjoitetun ja siirretyn aineiston oikeellisuus vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään.

2. Patenttivaatimuksen 1 mukainen menetelmä, tunnettu siitä, että

siirretään matkaviestimeen allekirjoitettavaksi siirretty aineisto toiselle osapuolelle; ja

allekirjoitettu aineisto toiselle osapuolelle, jolloin toinen osapuoli varmistaa allekirjoituksen oikeellisuuden.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, tunnettu siitä, että salataan aineisto ennen sen siirtämistä matkaviestimen ja toisen osapuolen välillä; ja

puretaan salaus ennen aineiston käsittelyä, kuten allekirjoitusta ja oikeellisuuden varmistamista.

4. Jonkin edeltävistä patenttivaatimuksista 1 - 3 mukainen menetelmä, tunnettu siitä, että

käytetään lomakkeen muodostamiseen ennalta sovitua tunnisteeellista lomakepohjaa, johon täydennetään

oleelliset tiedot ennen sen siirtämistä matkaviestimeen.

5 5. Jonkin edeltävistä patenttivaatimuksista 1
- 4 mukainen menetelmä, tunnettu siitä, että
muodostetaan tiiviste hash-funktiolla.

6. Jonkin edeltävistä patenttivaatimuksista 1
- 5 mukainen menetelmä, tunnettu siitä, että
käytetään viestin allekirjoitukseen ja/tai salaukseen julkisen ja salaisen avaimen menetelmää.

10 7. Jonkin edeltävistä patenttivaatimuksista 1
- 6 mukainen menetelmä, tunnettu siitä, että
esitetään aineisto ja/tai osa siitä matkaviestimessä ennen aineiston allekirjoittamista.

15 8. Jonkin edeltävistä patenttivaatimuksista 1
- 7 mukainen menetelmä, tunnettu siitä, että
käynnistetään matkaviestin allekirjoitusmodissa ennen aineiston siirtämistä matkaviestimeen.

20 9. Jonkin edeltävistä patenttivaatimuksista 1
- 8 mukainen menetelmä, tunnettu siitä, että
merkitään aineistoon aikaleima; ja
arkistoidaan aineiston allekirjoitustapahtumaisen jälkeen, kun allekirjoitus on todettu oikeaksi.

25 10. Järjestelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvalisesti matkaviestimellä (MS), johon järjestelmään kuuluu

30 maksuautomaatti (2);
maksuautomaattiin yhdistetyt välineet (3) allekirjoitettavan aineiston, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, muodostamiseksi; ja

35 maksuautomaattiin yhdistetyt välineet (4) aineiston siirtämiseksi matkaviestimeen (MS), tunnettu siitä, että

maksuautomaattiin kuuluu välineet (5) ensimmäisen tiivisteen (H1) laskemiseksi allekirjoitettavasta aineistosta;

matkaviestimeen kuuluu allekirjoitusvälineet
(6) siihen siirretyn aineiston allekirjoittamiseksi;
ja

5 maksuautomaattiin kuuluu välineet (7) alle-
kirjoitetun ja siirretyn aineiston oikeellisuuden var-
mistamiseksi vertaamalla allekirjoitettua tiivistet-
tä (H1_{as}) ja aineistosta ennen allekirjoitusta laskettua
tiivistettä (H1) keskenään.

10 11. Patenttivaatimuksen 10 mukainen järjes-
telmä, tunnettu siitä, että järjestelmään kuuluu
palvelin (8), joka on yhdistetty maksuauto-
maattiin (2) ja matkaviestimeen (MS) ja kolmannen osa-
puolen valvonnassa; ja

15 matkaviestimeen kuuluu välineet allekirjoite-
tun aineiston salaamiseksi.

12. Patenttivaatimuksen 10 tai 11 mukainen
järjestelmä, tunnettu siitä, että palvelimeen (8)
kuuluu

20 välineet (9) digitaalisen allekirjoituksen
oikeellisuuden todentamiseksi.

13. Jonkin edeltävistä patenttivaatimuksista
10 - 12 mukainen menetelmä, tunnettu siitä, että
matkaviestimeen kuuluu

25 välineet (10) aineiston ja/tai osan siitä
esittämiseksi matkaviestimessä ennen aineiston alle-
kirjoittamista.

14. Jonkin edeltävistä patenttivaatimuksista
10 - 13 mukainen menetelmä, tunnettu siitä, että
palvelimeen (8) kuuluu

30 välineet (11) aikaleiman merkitsemiseksi ai-
neistoon; ja

välineet (12) aineiston allekirjoitustapahtu-
man arkistoinniseksi sen jälkeen, kun allekirjoitus on
todettu oikeaksi.

(57) TIIVISTELMÄ

Menetelmä sähköisessä muodossa olevan lomakkeen digitaalseksi allekirjoittamiseksi turvallisesti matkaviestimellä. Menetelmässä siirretään allekirjoitettava aineisto, johon kuuluu lomake, sen tunnistetiedot, ja/tai siihen lisätyt olennaiset tiedot, matkaviestimeen, lasketaan allekirjoitettavasta aineistosta ensimmäinen tiivistelmä (H1), lisätään tiivistelmä aineistoon siirrettäväksi matkaviestimeen, allekirjoitetaan digitaalisesti matkaviestimellä siihen siirretty aineisto ja varmistetaan allekirjoitetun ja siirretyn aineiston oikeellisuus vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään. Keksinnön ansiosta matkaviestintä voidaan turvallisesti käyttää digitaaliseen allekirjoitukseen erilaisissa sovelluksissa.

(Fig. 1)

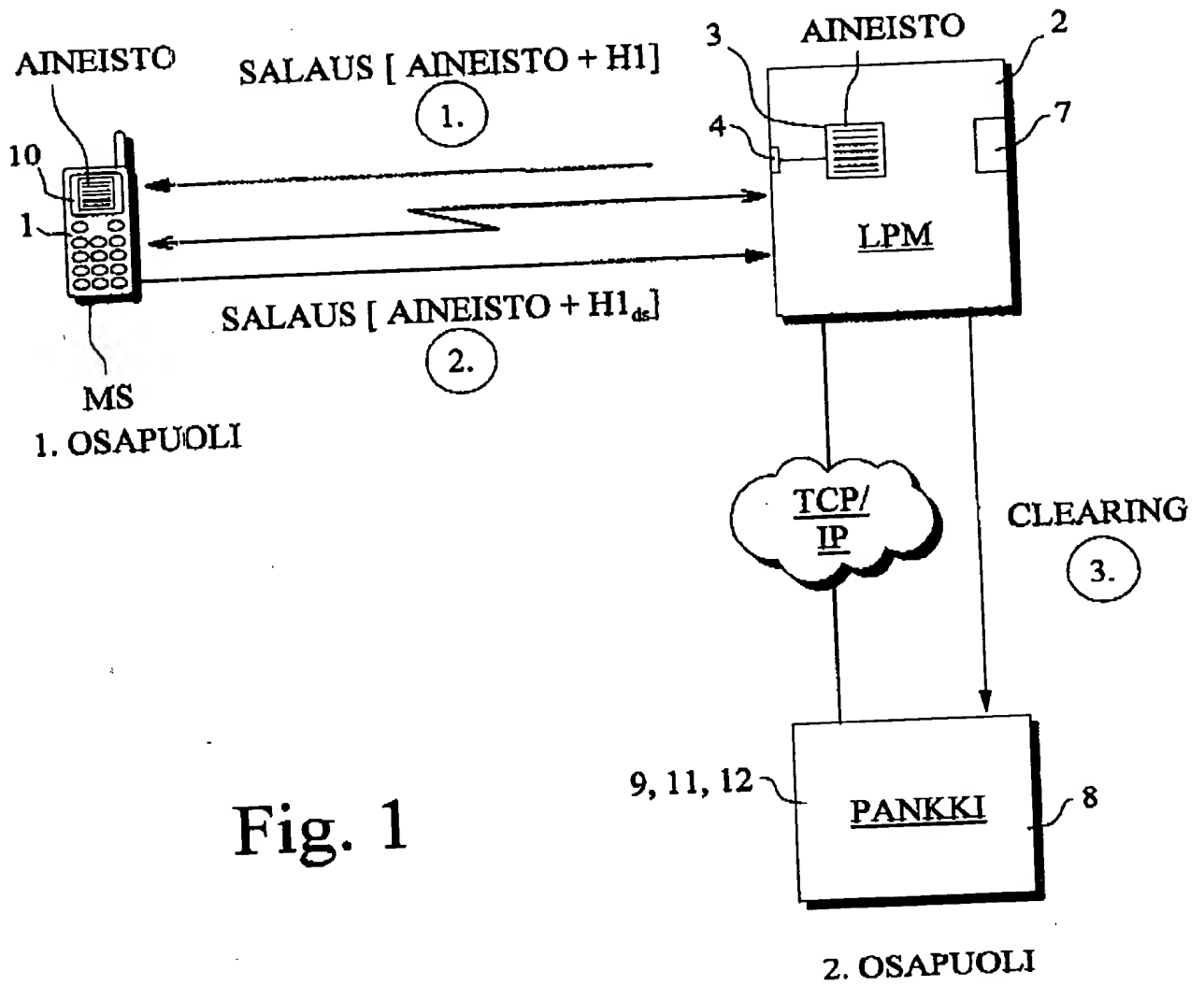


Fig. 1

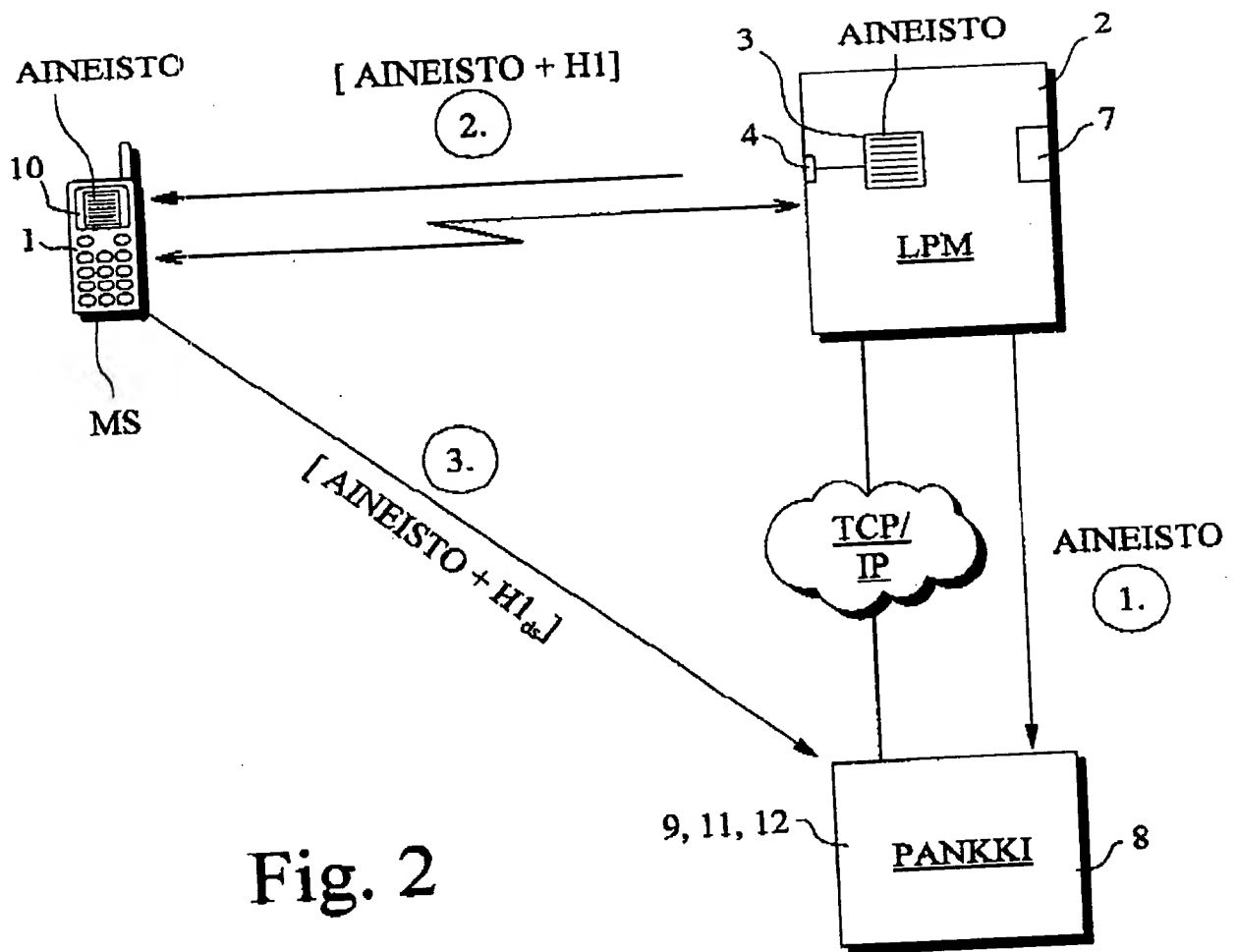


Fig. 2

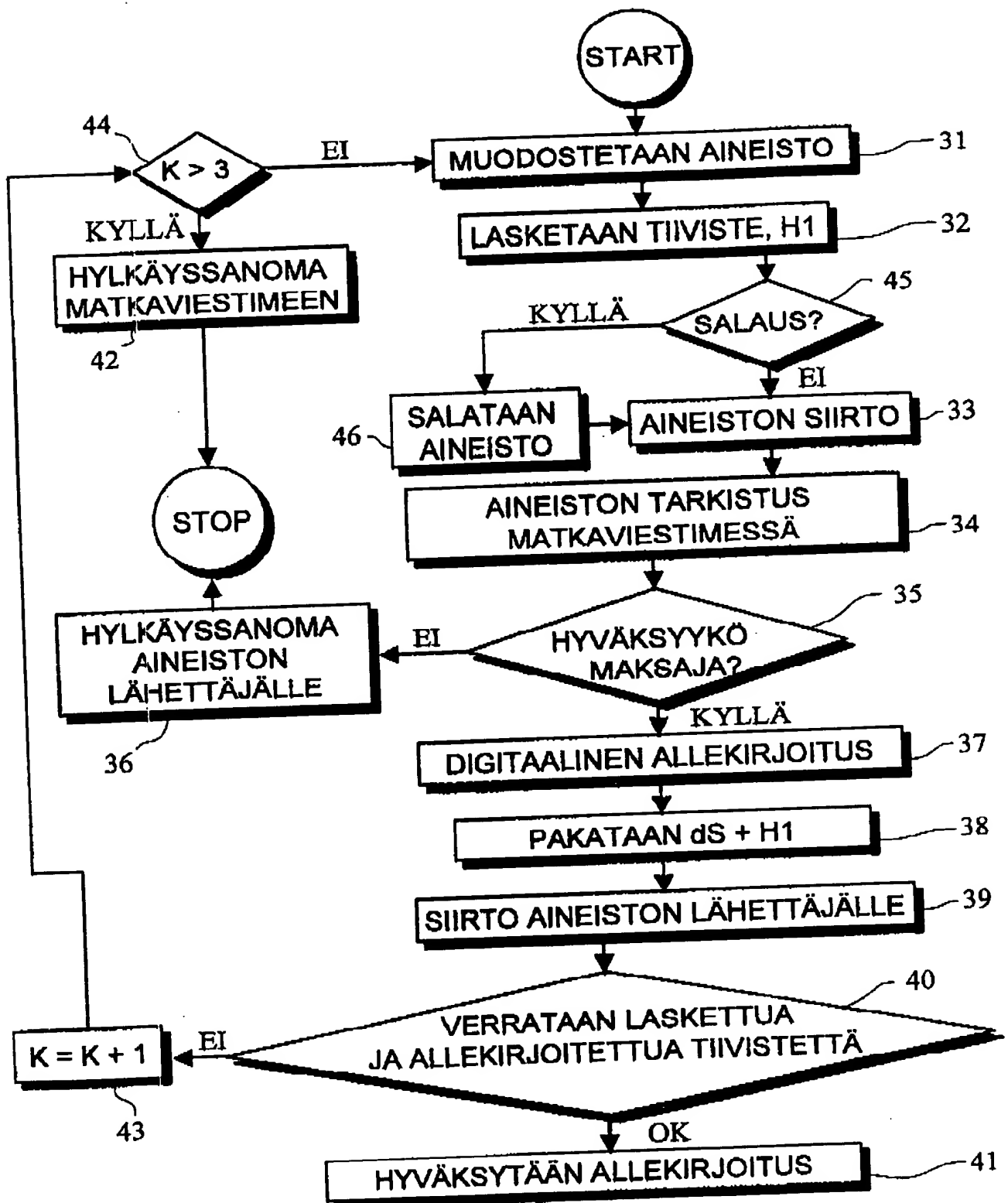


Fig. 3

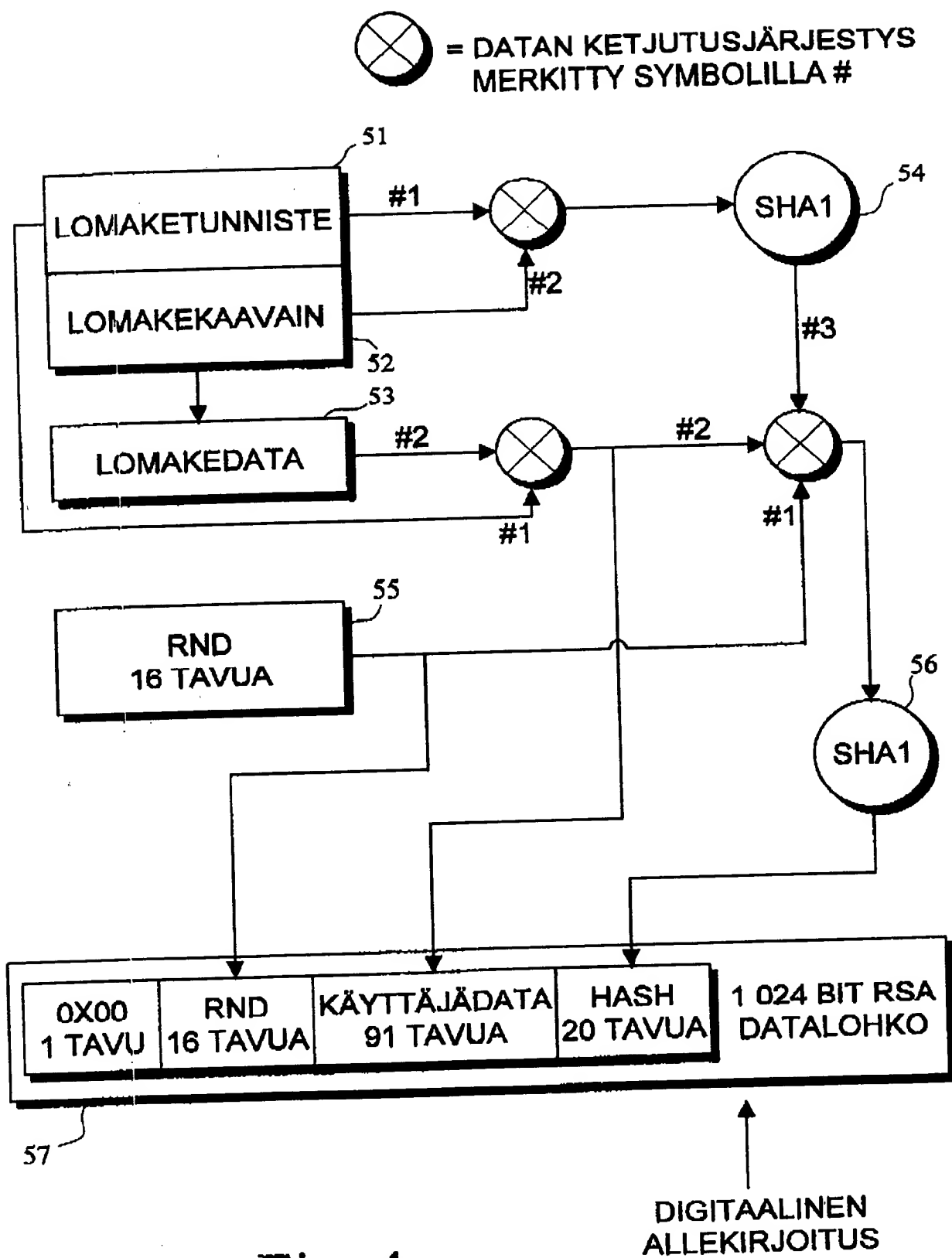


Fig. 4

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspio)